9110-9B P

DEPARTMENT OF HOMELAND SECURITY

Docket No. DHS-2017-0068

Privacy Act of 1974; System of Records

AGENCY: Department of Homeland Security.

ACTION: Notice of a Modified System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to modify and reissue a current Department of Homeland Security system of records titled, "Department of Homeland Security/ALL-039 Foreign Access Management System of Records." The Department of Homeland is updating this system of records notice to correctly reflect the categories of individuals impacted and modify the routine uses. This system of records allows the Department of Homeland Security to collect and maintain records on foreign nationals who request physical or information technology system access to the Department of Homeland Security and other U.S. Government partner agencies for which the Department of Homeland Security provides screening support. These individuals may include U.S. citizens and lawful permanent residents representing foreign interests; lawful permanent residents providing construction and contractual services for the Department of Homeland Security and other U.S. Government partner agencies; foreign visitors to fusion centers or tribal, territorial, state, and local government homeland security programs; and reported foreign contacts of Department of Homeland Security and other U.S. Government employees outside the scope of the employee's official activities required for personnel security purposes.

Additionally, the Department of Homeland Security is issuing a modified Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act, elsewhere in the Federal Register. This modified system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This modified system will be effective upon publication. New or modified routine uses will be effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number DHS-2017-0068 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Philip S. Kaplan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

Instructions: All submissions received must include the agency name and docket number DHS-2018-0009. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general and privacy-related questions, please contact: Philip S. Kaplan, (202) 343-1717, Privacy@hq.dhs.gov, Chief

Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) proposes to modify and reissue a current DHS system of records titled, "DHS/ALL-039 Foreign Access Management System of Records."

DHS is publishing this system of records notice (SORN) to update the categories of individuals and modify the routine uses. In the original SORN, the categories of individuals indicated that dual U.S. citizens and lawful permanent residents (LPR) representing foreign interests were included. This SORN is being updated to indicate that all U.S. citizens representing foreign interests are included in the categories of individuals, not just dual U.S. citizens. Routine use E, which deals with a suspected or confirmed breach of the system or information, has been modified and is now covered in routine uses E and F. This is to meet the requirements of OMB M-17-12. All subsequent routines uses have been re-lettered.

This SORN provides transparency on how DHS collects, uses, maintains, and disseminates information relating to foreign nationals who seek access to DHS and partner U.S. Government (USG) agency personnel, information, facilities, programs, research, studies, and information technology (IT) systems. The DHS Office of the Chief Security Officer (OCSO)/Center for International Safety & Security (CISS) Foreign Access Management (FAM) program uses the Foreign Access Management System (FAMS) to manage the risk assessment process for foreign nationals requesting access to

DHS and partner agencies. DHS is responsible for conducting screening of all foreign nationals and foreign entities seeking access to DHS personnel, information, facilities, programs, and IT systems, including: U.S. citizens and lawful permanent residents (LPR) representing foreign interests; and foreign contacts and foreign visitors reported by DHS. This SORN also covers the screening of LPRs who provide construction or contractual services (e.g., food services, janitorial services) to the U.S. Government, and DHS or USG federal employees that sponsor foreign national access to USG facilities or report foreign contacts who have met and/or befriended such contacts and visitors outside the scope of the employee's official duties.

As part of a government-wide pilot, DHS will also conduct foreign access management screening activities for federal agencies other than DHS participating in the pilot. DHS may also screen foreign visitors to fusion centers or tribal, territorial, state, and local government homeland security programs.

Lastly, DHS uses FAMS records to screen foreign contacts of DHS employees outside the scope of the employee's official activities. DHS and other USG employees and contractors with access to Sensitive Compartmented Information or other special program access have a responsibility to report all foreign contacts that are of a close, continuing personal association and any contacts with known or suspected intelligence officers from any country. Reporting of contact with foreign nationals is not intended to inhibit or discourage contact with foreign nationals. Rather, it permits the Government to manage and assess the risk posed by certain foreign individuals who seek to exploit personal relationships for purposes of collecting classified or sensitive information.

Foreign nationals accessing DHS or a partner USG agency in any of the capacities

listed above undergo DHS screening. In addition, foreign nationals may be screened as a result of foreign contact reporting for personnel security purposes. The foreign national screening process consists of both internal and external identity checks. The OCSO/CISS validates the foreign national identifying information provided.

DHS shares vetting, as well as any security anomalies or derogatory information identified through the vetting process, with DHS components and partner USG agencies. DHS will maintain information on any security incidents or suspicious activities recorded during the foreign national's access to DHS or partner USG agencies. The information is shared by secure means commensurate with the classification of the information to be shared.

Consistent with DHS's information sharing mission, information stored in the DHS/ALL-039 Foreign Access Management System of Records may be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice. However, to limit the scope of sharing with foreign partners, DHS will consider a foreign entity's ability to safeguard personally identifiable information (PII), and its commitment to and history of safeguarding such information, when determining whether to share records containing PII.

Additionally, DHS is issuing an updated Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act elsewhere in the

Federal Register. This modified system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, and similarly, the Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/ALL-039 Foreign Access Management System of Records.

In accordance with 5 U.S.C. sec. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER: Department of Homeland Security (DHS)/ALL-039 Foreign Access Management System of Records.

SECURITY CLASSIFICATION: Unclassified and Classified.

SYSTEM LOCATION: Records are maintained at the Department of Homeland Security Headquarters in Washington, D.C. and field offices. Electronic records are stored in the Integrated Security Management System (ISMS) as well as in a classified network database.

SYSTEM MANAGER(S): Director, Center for International Safety & Security, Office of the Chief Security Officer, Department of Homeland Security, 301 7th Street SW, D.C. 20024.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 301; 40 U.S.C. 1315; 40 U.S.C. 11331; the Economy Act of 1932, as amended; the Counterintelligence Enhancement Act of 2002; the Intelligence Reform and Terrorism Prevention Act; E.O. 12977; E.O. 13286; E.O. 13549; Presidential Policy Directive/PPD-21, "Critical Infrastructure Security and Resilience" (February 12, 2013); DCI Directive 6/4, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)" (July 2, 1998); and Presidential Decision Directive (PDD)/NSC- 12, "Security Awareness and Reporting of Foreign Contacts" (August 5, 1993).

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to perform screening for foreign nationals seeking access to DHS and partner USG agency personnel, information, facilities, programs, research, studies, and IT systems. This system is also used to screen foreign contacts and foreign visitors reported by DHS and partner USG agency employees who have met and/or befriended such contacts and visitors outside the scope of the employee's official duties.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Foreign nationals and foreign entities seeking access to USG personnel, information, facilities, programs, research, studies, and IT systems, including: U.S. citizens and lawful permanent residents (LPR) representing foreign interests; and foreign contacts and foreign visitors reported by DHS. These include, when requested, foreign visitors to fusion centers or tribal, territorial, state, and local government homeland security programs, and foreign contacts of USG employees who have met or befriended such contacts and visitors outside the scope of the employee's official duties. Further, DHS or USG federal employees that sponsor foreign national access to USG or report foreign contacts outside the scope of their normal employment duties. Finally, LPRs providing construction or contractual services (e.g., food services, janitorial services)

CATEGORIES OF RECORDS IN THE SYSTEM:

For foreign nationals:

- Full name;
- Alias(es);
- Gender;
- Date of birth;
- Place of birth;
- City/country of residence;
- Country of citizenship;
- Passport information (country of issue, number, expiration date);
- Passport copy;
- Photograph;

- Address;
- Telephone number(s);
- Email Address(es);
- Country sponsoring the visit;
- Stated reason for the visit;
- DHS component sponsoring the visit;
- Diplomatic identification information;
- Organization represented, title, or position held;
- Actual employment information (including job title and employer contact information);
- Visa information (type, number, expiration date, and issuance location);
- Foreign Access Management System number;
- Alien registration number; and
- Potential anomalous or derogatory information identified as part of screening and vetting results.

For USG federal employees:

- Full name;
- Title;
- Organization and component;
- Phone number; and
- Email address.

RECORD SOURCE CATEGORIES: DHS obtains information directly from the federal employee sponsor, and the DHS or USG employee providing the information to DHS for screening. DHS also obtains information from the other DHS and federal

systems for vetting purposes, including:

1. U.S. Customs and Border Protection (CBP) Advance Passenger Information System (APIS): DHS/CBP-005 APIS, 80 FR 13407 (March 13, 2015);
2. CBP Arrival and Departure Information System (ADIS): DHS/CBP-021 ADIS, 80 FR 72081 (November 18, 2015);
3. CBP Automated Targeting System (ATS): DHS/CBP-006 ATS, 77 FR 30297 (May 22, 2012);
4. CBP TECS: DHS/CBP-011 TECS, 73 FR 77778 (December 19, 2008).
5. U.S. Immigration and Customs Enforcement (ICE) Criminal Arrest Records and Immigration Enforcement Records (CARIER): DHS/ICE-011 CARIER, 81 FR 72080 (October 19, 2016); and
6. ICE Student and Exchange Visitor Information System (SEVIS): DHS/ICE-001 SEVIS, 75 FR 412 (January 5, 2010).
7. National Protection and Programs Directorate (NPPD) Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT): DHS/US-VISIT-004 DHS IDENT, 72 FR 31080 (June 5, 2007);
8. U.S. Citizen and Immigration Services (USCIS) Alien File, Index, and National File Tracking System (A-File): DHS/USCIS/ICE/CBP-001 A-File, 82 FR 43556 (September 18, 2017);
9. USCIS Benefits Information System (BIS): DHS/USCIS-007 BIS, 81 FR 72069 (October 19, 2016);

DHS also obtains information from intelligence community classified systems for screening and vetting.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including the U.S. Attorneys Offices, or other federal agency conducting litigation or proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity, only when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. sec. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To another Federal agency or Federal entity, when DHS determines that information from this system of records is reasonably necessary and otherwise compatible with the purpose of collection to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

G. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records.

H. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory

violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

I. To federal and foreign government intelligence or counterterrorism agencies or components when DHS becomes aware of an indication of a threat or potential threat to national or international security, or when such use is to conduct national intelligence and security investigations or assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

J. To federal government intelligence or counterterrorism agencies or components to facilitate CISS screening checks.

K. To other federal agencies to assist in their determination of whether to grant a requesting foreign national with access to that federal agency.

L. To appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, when DHS is aware of a need to use relevant data for purposes of testing new technology.

M. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: DHS stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by foreign contact or USG employee name, or other personal identifiers listed in the categories of records, above.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: In accordance with NARA-approved retention schedule N1-563-09-1, DHS retains information collected on foreign visitors for screening in FAMS and in the Classified Local Area Network (C-LAN) access database for twenty years.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES: The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and consequently those of the Judicial Redress Act if applicable. However, DHS will consider individual requests to determine whether or not information may be released. Thus, individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing

to the Chief Privacy Officer and Chief Freedom of Information Act (FOIA) Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contacts Information." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief FOIA Officer, Department of Homeland Security, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about you may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, an individual may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, the individual should:

- Explain why you believe the Department would have information on him/her;
- Identify which component(s) of the Department the individual believes may have the information about him/her;
- Specify when the individual believes the records would have been created; and

- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If an individual's request is seeking records pertaining to another living individual, the first individual must include a statement from the second individual certifying his/her agreement for the first individual to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES: For records covered by the Privacy Act or covered JRA records, see "Record Access Procedures" above.

NOTIFICATION PROCEDURES: See "Record Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: The Secretary of Homeland Security, pursuant to 5 U.S.C. 552a(k)(1), (k)(2), and (k)(5), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f). When this system receives a record from another system exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

HISTORY: DHS/ALL-039 Foreign Access Management System of Records, 82 FR 34971 (July 27, 2017).

Philip S. Kaplan,
Chief Privacy Officer,
Department of Homeland Security.

[FR Doc. 2018-09196 Filed: 4/30/2018 8:45 am; Publication Date: 5/1/2018]